9 FAM 40.37 NOTES

(CT:VISA-741; 06-03-2005)
(Office of Origin: CA/VO/L/R)

9 FAM 40.37 N1 "VISAS VIPER" TERRORIST REPORTING PROGRAM

9 FAM 40.37 N1.1 Background and Purpose

(CT:VISA-741; 06-03-2005)

a. The VISAS VIPER Program (VVP) originated in response to the 1993 World Trade Center (WTC) bombing and other threats and incidents of terrorism involving foreign nationals. An investigation into the WTC bombing revealed deficiencies in the way available information on terrorists was being shared at posts abroad and reported to the Department. Specifically found lacking, was a mechanism for routinely and consistently bringing suspected terrorists to the Consular Section's attention for the purpose of entering their names into the Department's "Consular Lookout and Support System" (CLASS) and into the Department of Homeland Security's (DHS) Customs and Border Protection's (CBP) "Interagency Border Inspection System" (IBIS). The VISAS VIPER Program was created to address this concern. Its mission is to:

(1) Utilize the cooperative resources of all elements of Foreign Service posts to identify potential terrorists;

(2) Develop information on such individuals;

(3) Provide a direct consular channel for reporting this information; and,

(4) Watchlist the subjects in CLASS and IBIS to ensure they are appropriately screened should they later apply for visas or for entry into the United States.

b. In May 1997, the TIPPIX Program was initiated to scan the photographs of suspected terrorists, obtained from Foreign Service posts and other sources, into the TIPOFF/VIPER counterterrorism database and the IBIS lookout system. In April 1998, the Department began sharing names

from the database with the Canadian Government under a program called TUSCAN. In 2000, prior to the Sydney Olympics, the Department began sharing names from the database with the Australian government under a program called TACTICS. Each program has significantly enhanced U.S. border security.

9 FAM 40.37 N2 SCOPE OF THE PROGRAM

9 FAM 40.37 N2.1 Limited to Non-Visa Applicants

(CT:VISA-741; 06-03-2005)

The VISAS VIPER Program (VVP) is intended solely for reporting on aliens who are not currently applying for U.S. visas. Visa applicants who are suspected of terrorist activity continue to be subject to the VISAS DONKEY or VISAS BEAR security advisory opinion (SAO) requirement. (See 9 FAM 40.37 N3.)

9 FAM 40.37 N2.2 Limited to Terrorists

(CT:VISA-741; 06-03-2005)

The VIPER channel is further limited to aliens who are known as potential terrorists. It should not be used to report on narcotraffickers, international criminals, or other malefactors unless they are also suspected of falling within the purview of INA 212(A)(3)(B) or INA 212(A)(3)(F).

NOTE: An alien who is not a current visa applicant, but whom a consular officer suspects of involvement in exclusionary criminal or narcotics trafficking activity, may be entered directly into CLASS by the consular post using the appropriate quasi refusal code. (See 9 FAM Appendix D Exhibit 1)

9 FAM 40.37 N3 DISTINCTION BETWEEN "VISAS VIPER" AND "VISAS DONKEY/BEAR"

(CT:VISA-741; 06-03-2005)

a. The VISAS VIPER reporting program complements the VISAS DONKEY and VISAS BEAR security advisory opinion (SAO) procedures.

b. VISAS VIPER telegrams report on possible terrorists who are not current visa applicants for the purpose of watchlisting them.

c. VISAS DONKEY and VISAS BEAR cables are used to request SAOs on such individuals when they apply for visas. Posts must use whichever procedure is appropriate to bring to the Department's attention all terrorists on whom they have information.

9 FAM 40.37 N4 VVP ADMINISTRATION AT FOREIGN SERVICE POSTS

9 FAM 40.37 N4.1 VISAS VIPER Committees

(CT:VISA-741; 06-03-2005)

a. The VVP is primarily administered at posts abroad through a VISAS VIPER Committee established at each post, chaired by the DCM or principal officer and composed of representatives from appropriate post entities. All sections and agencies involved in security, law enforcement, and intelligence activities should participate, as should those having official and/or public contacts that may produce terrorism-related information. The VISAS VIPER Committees meet at least monthly to share information on known or suspected terrorists and to determine whether such information meets the criteria for VISAS VIPER reporting. (See 9 FAM 40.37 N7.)

b. A report summarizing the results of the committee meeting(s) held during each month is required in accordance with the instructions. (See 9 FAM 40.37 N6.) While VISAS VIPER Committee meetings are the principal forums for sharing terrorist intelligence at post, information developed on an ad hoc basis, particularly that of an urgent nature, must also be considered for expeditious reporting through the VISAS VIPER channel.

9 FAM 40.37 N4-2 Post VVP Coordinators

(CT:VISA-741; 06-03-2005)

Posts are encouraged to designate a VISAS VIPER Coordinator, normally the consular section chief or an officer responsible to him or her, who would serve the following functions:

(1) Serve as liaison with other sections and agencies (provide information and advice on VVP policies and procedures, ensure that State Department officers use the VISAS VIPER channel when reporting on terrorists, and promote awareness and utilization of the VIPER channel among other-agency representatives);

(2) Coordinate VIPER committee meetings (assist the DCM/PO in scheduling the mandatory monthly meetings and arrange appropriate State Department and other-agency participation);

(3) Oversee VISAS VIPER reporting (prepare required monthly reports on post's VVP activities and monitor ad hoc reporting on individual terrorists); and

(4) Serve as liaison with the Department (maintain contact with the Department's VISAS VIPER Coordinator, seek guidance on questions regarding VVP issues, and respond to the Department's requests for information on VIPER cases).

9 FAM 40.37 N5 VVP ADMINISTRATION WITHIN WASHINGTON

(CT:VISA-741; 06-03-2005)

a. The VISAS VIPER Program is an integral part of "TIPOFF", a program that coordinates the use of interagency intelligence for the watchlisting of terrorists. TIPOFF is located in the National Counterterrorism Center (NCTC) (previously the Terrorist Threat Integration Center (TTIC) and Terrorist Screening Center (TSC)). VISAS VIPER continues to be managed by the Department of State. TIPOFF maintains a counterterrorism database now numbering over 88,000 names, of which more than 43,000 were contributed through the VISAS VIPER channel. The TIPOFF/VIPER staff, in close cooperation with the Visa Office's Coordination Division (CA/VO/L/C):

(1) Develops VISAS VIPER policies and procedures, creates and updates TIPOFF records; and

(2) Determines whether the names of individual suspected terrorists are entered into CLASS and IBIS.

(3) Provides feedback and guidance to Foreign Service posts on VISAS VIPER reporting;

(4) Serves as liaison with interested offices in the Department and with the headquarters of other government agencies on matters relating to the program.

b. Correspondence, including hard copies of photographs and news articles, should be sent to the VISAS VIPER staff at NCTC, Room 4G20 OHB, Washington, DC 20505. E-mail to the VISAS VIPER staff can be sent via the Department's unclassified or classified systems. Classified material

can be sent via Department pouch. The VISAS VIPER Operational Administrator can be reached telephonically at (703) 482-9731. Faxes may be sent to (703) 482-4446 (unclassified) and (703) 482-3713 (classified).

9 FAM 40.37 N6 VISAS VIPER MONTHLY REPORTING REQUIREMENT

9 FAM 40.37 N6.1 Mandate and Contents

(CT:VISA-741; 06-03-2005)

In August, 2002, Posts began submitting mandatory monthly reports (in place of the former quarterly requirement), outlining their VISAS VIPER Program activities during each period. Such reports should contain the date(s) VVP Committee meetings were held, the number of VIPER telegrams submitted (including cable references), and a brief discussion of any questions or comments the post may have regarding the program's policies and procedures. These mandatory reports must be submitted even if no information on terrorists was developed during the month. The monthly report requirement provides the basis for the quarterly reports to Congress that the Department is now required to make under Section 304 of the Enhanced Border Security and Visa Entry Reform Act of 2002.

9 FAM 40.37 N6.2 Preparation of Monthly Reports

(CT:VISA-741; 06-03-2005)

VVP quarterly reports are due no later than ten (10) days following the end of the previous month, i.e., the February report is due by March 10. The format for the report is described in 9 FAM 40.37 N10.

9 FAM 40.37 N6.3 Submitting Monthly Reports for Other Posts

(CT:VISA-741; 06-03-2005)

We are aware that some posts are consulting with and submitting monthly reports on behalf of constituents and/or non visa-issuing posts within their host countries. In such cases, the reporting posts should be certain to indicate clearly in their monthly reports the posts with which they have consulted on VISAS VIPER activities and on whose behalf they are reporting.

"Virtual" coordination meetings between posts are also acceptable and encouraged for smaller constituent posts.

9 FAM 40.37 N7 VISAS VIPER REPORTING CRITERIA

(CT:VISA-741; 06-03-2005)

a. A VISAS VIPER cable must be submitted if:

(1) There is reason to suspect that an individual falls within the purview of INA 212(A)(3)(B) **or** INA 212(A)(3)(F); and,

(2) There is sufficient biographic data to positively identify the subject of the information. Key identifying data are name (including aliases), date of birth, and passport information (country of issue/number).

b. The primary goal of the VISAS VIPER Program is to develop high quality, usable records on possible terrorists, not merely to collect impressive statistics. A VISAS VIPER telegram should, therefore, only be sent if both of the above criteria are met.

9 FAM 40.37 N7.1 Reason to Suspect Terrorist Activity

(CT:VISA-741; 06-03-2005)

a. The information provided in a VISAS VIPER telegram must be sufficient to sustain a reasonable suspicion that the individual is subject to INA 212(A)(3)(B) or could appropriately be subject to a determination of the Secretary under INA 212(A)(3)(F). The authority of Section INA 212(A)(3)(B)(IV)(BB), INA 212(A)(3)(B)(VI), and INA 212(A)(3)(F) is not vested in consular officers and can only be exercised by the Secretary or officials to whom he or she has delegated his or her authority. Section INA 212(A)(3)(F) may also be invoked by the Secretary of Homeland Security. Section INA 212(A)(3)(B) has become extremely broad and complex and should be carefully reviewed regularly by all members of the VISAS VIPER Committee to ensure that all understand the full scope of the provision. It encompasses, but is not limited to, any person who:

(1) Has engaged, is engaged, or is likely to engage in terrorist activity as defined in that section

Note: Terrorist activity and engaging in terrorist activity are both defined terms and are defined very broadly.

(2) Has incited terrorist activity with intent to cause death or bodily harm; or,

(3) Is a member or representative of a terrorist organization designated under Section 219 of the INA (the "Foreign Terrorist Organizations") or is a knowing member of such an organization. The names of the terrorist organizations can be found on the Department's Foreign Terrorist Listings.

b. It should be noted that the "reasonable suspicion" criterion for submitting VISAS VIPER cables represents a lesser standard than the "reason to believe" standard, required to support visa denial under certain subsections of INA 212(A)(3)(B). We consider the "reasonable suspicion" criterion to be met if the derogatory information currently available would warrant further detailed inquiry into the subject's background should he or she apply for a visa. An individual's association with known or suspected terrorists or terrorist groups also meets the criterion if such association suggests a proscribed membership or personal involvement in terrorist acts or that the person could fall within the scope of the authorities in INA 212(A)(3)(B), or INA 212(A)(3)(B)(IV) that are committed to the Secretary.

9 FAM 40.37 N7.2 Identification of Subject

(CT:VISA-741; 06-03-2005)

a. It is essential to develop and report all available identifying data on the subjects of VISAS VIPER telegrams. Derogatory information on a suspected terrorist, regardless of its gravity, is of little value unless it can be linked to that individual should he or she apply for a visa or for entry into the United States. Insufficient biographic data in a given case can result in a failure to identify a serious threat to U.S. security. It can also produce "false hits" which complicate visa adjudication, and cause unwarranted inconvenience to bona fide visa applicants. For these reasons, we carefully weighs the adequacy of biographic information when determining whether to create TIPOFF records and CLASS and/or IBIS entries on the subjects of VISAS VIPER reporting. It should be noted, however, that even when CLASS and IBIS entries are not made because of insufficient biographic data, TIPOFF records are often created on the subject in case additional information is later developed.

b. VISAS VIPER telegrams should ideally provide full names (including

aliases and alternate spellings) and dates and places of birth. Since naming conventions vary by country and region, the subject's surname(s) must be clearly identified, either by listing it and/or them first, followed by a comma and the given name(s), or by placing the surname(s) in parentheses. In cases where the subject's given name can be either masculine or feminine, the subject's gender should be specified.

c. If an individual's exact date and place of birth are not available, a reasonable estimate of his or her age and the known or probable country of birth should be provided if possible. VISAS VIPER telegrams may be submitted without birth data if the subject's name is not a common one, and if the post is able to provide other identifying information. Personal details such as passport data, physical characteristics, education, profession, residential and employment history, and the names of family members are often useful in establishing identity. A subject's affiliation with a terrorist group, and his or her position therein, should always be reported, as this information is particularly valuable for both identification and threat assessment purposes.

d. Please note that a year of birth, at a minimum, is required to enter a subject's name into the CBP IBIS lookout system. It is especially important to keep this in mind when reporting on nationals of visa waiver countries since the only screening of such individuals is through IBIS at U.S. ports-of-entry (POE).

9 FAM 40.37 N8 PRIORITIZING AND EVALUATING TERRORIST INFORMATION

9 FAM 40.37 N 8.1 Priorities for Terrorist Reporting

(CT:VISA-741; 06-03-2005)

While all suspected terrorists meeting the VISAS VIPER criteria must be reported, posts should keep in mind the following priorities when gathering and evaluating terrorist information. These priorities, ranked in descending order of threat, were developed in consultation with other U.S. Government agencies:

(1) Individuals who pose or may pose a present threat to U.S. interests in the United States or abroad;

(2) Individuals who are not known to pose a present threat to U.S. interests, but who have done so within the past 15 years; and,

(3) Individuals not in categories (1) or (2) but who pose a present threat to non-U.S. interests, or who have posed such a threat within the past ten years.

9 FAM 40.37 N8.2 Evaluation of Terrorist Information

(CT:VISA-741; 06-03-2005)

a. The following factors are among many that must be considered when evaluating terrorist information and/or assessing its urgency:

(1) The immediacy and severity of the threat posed;

(2) The reliability of the information;

(3) Whether the subject is clearly identified; and

(4) Whether additional information could be developed within a reasonable time period to further clarify the situation or better identify the subject.

b. Evaluating terrorist information for the purpose of submitting VISAS VIPER reporting requires the sound exercise of judgment because not all information can be anticipated or made subject to predetermined clear guidelines. We believe that each post's VISAS VIPER Committee, which has first-hand knowledge of the host country's terrorist threat situation, should be well-positioned to exercise such judgment and generally will be better positioned to do so than the Department. If the post believes the reporting criteria outlined in 9 FAM 40.37 N7 has been met, a VISAS VIPER telegram providing all known information should be submitted.

c. Posts are urged to draw on all sources to develop information on suspected terrorists, including open source reporting. While VISAS VIPER coordinators are usually within the consular section, the political, economic and public affairs sections can be assigned primary responsibility for collecting open source terrorist biographic information as a general rule. Posts are requested to periodically review which elements in the mission have the best access and capability to obtain terrorist information from the host country. Whichever section is given the lead, it remains crucial that all mission elements participate in and contribute to the work of posts' VISAS VIPER committees.

9 FAM 40.37 N9 VISAS VIPER REPORTING CHANNEL

(CT:VISA-741; 06-03-2005)

a. Counterterrorism reporting is an important foreign policy function, requiring the collaborative effort of all members of a post's country team. Except in the rare instances where there are special operational concerns, all State Department reporting on terrorists, including Diplomatic Security (DS) reporting, should be transmitted through the VISAS VIPER channel.

b. Other agency terrorist reporting may use the VIPER channel or be sent through the agency's traditional reporting channel. Regardless of the means of transmission chosen, it is essential to ensure that suspected terrorists are screened for possible inclusion in the CLASS and IBIS lookout systems. When other channels are used, the inclusion of the "VISAS VIPER" term, either as a caption ("For VISAS VIPER") or passing instruction (Pass to State for VISAS VIPER) will facilitate receipt by TIPOFF staff.

c. Post's monthly VISAS VIPER report can also be used to alert the Department to other agency reporting, for example by simply listing an individual and noting that "additional information reported via other channels".

9 FAM 40.37 N9-1 Departmental Reporting

(CT:VISA-741; 06-03-2005)

a. The VISAS VIPER channel offers a direct consular conduit for watchlisting known and suspected terrorists and must be used for all Departmental reporting on individuals who meet the VIPER Program's scope and criteria. Information on terrorists may originate from a variety of sources including consular interviews, media reporting, security officer contacts, and from other post sections and agencies.

b. The Foreign Broadcast Information Service (FBIS), if available at post, is a valuable resource. While one section of the Post, normally the Consular Section, has responsibility for coordinating and monitoring VISAS VIPER reporting, other Department sections are responsible for sharing terrorist information with that section, and, if drafting reports on terrorists, for ensuring that such reporting is transmitted through the VISAS VIPER channel. For procedural guidance on preparing VISAS VIPER telegrams,

refer to 9 FAM 40.37 N10.

c. Finally, VISAS VIPER telegrams should include:

(1) An evaluation of the credibility;

(2) The applicability of the information submitted;

(3) A general description of the source; and

(4) An assessment of the source's reliability.

9 FAM 40.37 N9-2 Other Agency Reporting

(CT:VISA-741; 06-03-2005)

a. Other agencies ideally will share terrorist information with the post's VISAS VIPER Committee for transmission to the Department through the VIPER channel. However, they may choose to send it directly to their headquarters (originating agencies may prefer to use their own reporting channels for a variety of reasons, including the protection of sources and methods). However, it is imperative, that one way or another, this information is reported to Washington to be considered for inclusion in the border security databases.

b. Currently, data transmitted to other agency headquarters is usually passed to the Department via the National Counter Terrorism Center (NCTC) for possible CLASS and IBIS entry. To ensure that the relevant headquarters do not inadvertently overlook the border security significance of such information, other-agency drafters should be asked to include in their terrorist reporting to their headquarters, the phrase "recommended for consideration in the VISAS VIPER program" in the text of outgoing messages.

c. At the same time, all post agencies should be made aware of the availability of the VISAS VIPER channel as a direct and expeditious means of watchlisting suspected terrorists in CLASS and IBIS, and should be encouraged to use it in all appropriate circumstances. Above all, we must do everything possible to ensure that a visa is not issued to a terrorist because of failure to watchlist aliens when relevant information was available.

9 FAM 40.37 N10 PREPARING VIPER TELEGRAMS

9 FAM 40.37 N10.1 Telegram Format

(CT:VISA-741; 06-03-2005)

VISAS VIPER submissions and status reports should be submitted to the Department. The month reported upon should be clearly identified in the subject line: e.g. "VISAS VIPER: FEBRUARY 2004 MONTHLY ACTIVITY REPORT." The reports should use the following tags:

- KVPR
- CVIS
- CMGT
- PINR
- PTER
- ASEC

Cables should be slugged for INR/TIPOFF and CA/VO/L/C and must be also be addressed to the following agencies:

- FBI WASHINGTON DC//INTD//CTD//CT WATCH//
- CIA WASHINGTON DC, NCTC WASHINGTON DC//TIG//
- US CUSTOMS AND BORDER PROTECTION, HOMELAND SECURITY CENTER WASHINGTON DC
- DIRNSA FORT GEORGE G MEADE MD; and
- DIA WASHINGTON DC.

9 FAM 40.37 N10.2 CLASS Checks and Classification

(CT:VISA-741; 06-03-2005)

a. Prior to submitting a VISAS VIPER telegram on a potential terrorist,

consular posts must conduct a CLASS check to determine whether the subject was previously included as a DPT-00 entry or under another code requiring a security advisory opinion (SAO). The VISAS VIPER telegram should be submitted notwithstanding a previous entry, since the information available to Post is likely to add to the subject's existing record. The results of the Class check should be reported in the Viper cable. Any Class entries must be fully cited so that the subject may be accurately identified and his/her record expeditiously located.

b. VISAS VIPER cables should be classified at an appropriate level and assigned appropriate telegraphic precedence. In a classified VIPER telegram, the portion containing the subject's name, date and place of birth, nationality, and passport number should remain unclassified since these data elements will likely be entered into the unclassified CLASS and IBIS lookout systems. All other information is protected according to its classification. Do not use either DS or ROGER channels when sending VISAS VIPER cables, since telegrams so transmitted require special handling that could delay processing.

9 FAM 40.37 N11 WATCHLISTING TERRORISTS

(CT:VISA-741; 06-03-2005)

The subjects of VISAS VIPER reporting who, after TIPOFF review, meet the program criteria are entered into TIPOFF's counterterrorism database and their names are included in CLASS under the DPT-00 code. As with all DPT-00 entries, the Department's security advisory opinion is required should a subject later apply for a visa, and no visa may be issued until the Department's response to the SAO request is received. The names of most individuals whose dates of birth are known are also entered into the IBIS lookout system. As indicated in to 9 FAM 40.37 N7.2 (d) east the subject's year of birth is needed to create an IBIS entry, making the provision of this information particularly important when submitting a VISAS VIPER cable on nationals of visa waiver countries.

9 FAM 40.37 N11.1 CLASS Entry by Posts in Certain Cases

(CT:VISA-741; 06-03-2005)

When a consular officer believes that a suspected terrorist should be included in CLASS immediately, the consular officer should enter the

subject's name directly using the appropriate quasi INA 212(a)(3)(B) refusal code "P3B". (See *9 FAM Appendix D Exhibit 1*) Circumstances requiring such action include, but are not limited to, a credible imminent threat to U.S. interests or an impending application for a U.S. visa by the subject. The consular officer must then expeditiously submit a VISAS VIPER telegram, in which the post's CLASS entry should be reported.

9 FAM 40.37 N11.2 Removing VVP CLASS and IBIS Entries

(CT:VISA-741; 06-03-2005)

Recommendations to delete CLASS and IBIS entries, which were based upon VISAS VIPER reporting, should be submitted to the Department slugged for INR/TIPOFF and CA/VO/L/C. The cable should contain the "VISAS VIPER" code indicator and the "KVPR" tag. Justification for the deletion request must be provided. Circumstances creating the need for such a recommendation might include the subject's demise or the development of evidence that the derogatory information against the subject, previously believed credible, is without foundation.

9 FAM 40.37 N12 DEPARTMENT FEEDBACK

(CT:VISA-741; 06-03-2005)

The Department will reply in a timely manner to all VISAS VIPER communications with the exception of routine monthly reports. We will inform posts regarding whether it has watchlisted each individual reported by post through VISAS VIPER channels for possible watchlisting, and will advise if additional information is needed. Posts' inquiries regarding VISAS VIPER policies and procedures will also receive the Department's prompt attention. We will make every effort to provide comprehensive guidance and feedback on VISAS VIPER matters to maintain a true partnership with Foreign Service posts in fulfilling this crucial counterterrorism responsibility.